AMENDMENTS TO THE CLAIMS

1.   (Currently Amended)   A system for authenticating the identity of one of a plurality of individuals each having communication devices that are communicatively linked via a public communications system wherein the individual is seeking access to at least one secure component having an input <u>wherein the input permits access to the at least one secure component when the individual inputs an input code in a first format</u>, the system comprising:

at least one record that includes information about each of the plurality of individuals, the information including a communication path which defines how to contact the individual's communication device and further defines a security protocol for allowing access to the <u>at least one</u> secure component wherein the security protocol further defines whether the individual can access the secured component via an alternative path incorporating the individual's communication device;

a controller having access to the at least one record wherein the controller receives signals from the input of the at least one secure component in response to the individual manipulating the input device indicating the individual seeks alternative access to the at least secured component, wherein the controller, in response to one of the individuals seeking access to the at least one secure component, retrieves the security protocol and communications path from the at least one record; and

a communications interface that allows signals between the communications device carried by the individual and the controller wherein the controller (i) evaluates the signal received from the input device of the secure component, (ii) sends a first signal to the communications device of the individual via the public communications system in response to the individual seeking access to the at least one secure component wherein the first signal includes a uniquely generated code that is to be input by the individual via the input <u>in the first format</u> and (iii) evaluates a response signal via the secured component by the individual by comparing the response signal to the security protocol to determine whether to allow alternative access by the individual to the at least one secure component.

2. (Original) The system of Claim 1, wherein the security protocol comprises sending a prompt signal to the individual via the communications interface prompting the individual to enter and transmit an access code using the communications device and then comparing the access code to a pre-recorded access code stored in the at least one record to ascertain whether the individual correctly entered and transmitted the access code.

3. (Original) The system of Claim 2, wherein the at least one record further includes additional security criteria and wherein the controller allows access to the at least one secure component only when the individual has satisfied the security protocol and the additional security criteria.

4. (Original) The system of Claim 3, wherein the additional security criteria includes location information from which the individual must send the access code and wherein the individual's communication device transmits location information when transmitting the access code to the communications interface such that the controller can evaluate the additional security criteria.

5. (Original) The system of Claim 1, wherein the security protocol comprises sending an access code to the user via the communications interface and then evaluating whether the individual correctly entered the access code on the input of the at least one secure component.

6. (Original) The system of Claim 5, wherein the security protocol comprises (i) sending a prompt signal to the individual via the communications interface prompting the individual to enter and transmit a first access code using the communications device, (ii) comparing the first access code to a pre-recorded access code stored in the at least one record to ascertain whether the individual correctly entered and transmitted the first access code, (iii) sending a second access code to the communications device in response to determining that the individual correctly entered and transmitted the first access code, and (iv) evaluating whether the individual successfully entered the second access code on the input of the secure component before allowing access to the secure component..

7. (Original) The system of Claim 1, wherein the communications interface comprises a modem that is adapted to provide cellular telephone communication between the controller and cellular telephone devices carried by the plurality of individuals.

8.   (Original) The system of Claim 1, wherein the at least one record further includes supplemental commands and corresponding actions wherein the controller, in response to receiving a supplemental command from a user, induces the system to implement the corresponding action.

9.   (Original) The system of Claim 8, wherein the supplemental command comprises an additional access code provided to the controller via the communications interface by the individual communications device.

10.   (Original) The system of Claim 9, wherein the supplemental command induces the controller to limit access to the at least one secure component.

11.   (Original) The system of Claim 1, wherein the controller is adapted to remotely enable the secure component when the controller receives an enablement signal from the individual via the communications interface.

12.   (Original) The system of Claim 11, wherein the controller remotely enables the secure component by sending a wake-on-LAN signal to the at least one secure component.

Claims 13-30 (Cancelled)